Notice of References Cited	Application/Control No. 10/046,224	Applicant(s)/Patent Under Reexamination NISHIOKA ET AL.	
	Examiner David G. Cervetti	Art Unit 2136	Page 1 of 3

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
	A	US-6,697,488	02-2004	Cramer et al.	380/30
	B	US-6,081,598	06-2000	Dai, Wei	380/28
	C	US-6,236,729	05-2001	Takaragi et al.	380/286
	D	US-5,297,206	03-1994	Orton, Glenn A.	380/30
	E	US-5,606,617	02-1997	Brands, Stefanus A.	380/30
	F	US-6,353,888	03-2002	Kakehi et al.	713/168
	G	US-2002/0044653	04-2002	Baek et al.	380/42
	H	US-5,987,133	11-1999	Aisaka, Kazuo	713/170
	I	US-6,813,358	11-2004	Di Crescenzo et al.	380/280
	J	US-5,365,589	11-1994	Gutowitz, Howard A.	380/43
	K	US-6,859,533	02-2005	Wang et al.	380/28
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N	EP 924895 A2	06-1999	European Patent	UCHIYAMA et al.	H04L 09/30
	O	JP 2000216774 A	08-2000	Japan	ABE, MASAYUKI	H04L 09/32
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	Neal Koblitz, Elliptic Curve Cryptosystems, Jan 1987, Mathematics of Computation, vol 48, nbr 177, pages 203-209.
	V	Naor et al., Public-key cryptosystems provably secure against chosen ciphertext attacks, 1990, ACM Press, pages 427-437.
	W	Michael Rabin, Digitalized signatures and public key functions as intractable factorization, Jan 1979, MIT Lab for Computer Science.
	X	Anand Desai, New Paradigms for Constructing Symmetric Encryption Schemes Secure against Chosen-Ciphertext Attack, 2000, Springer-Verlag, CRYPTO 2000, pp 394-412.

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Notice of References Cited	Application/Control No. 10/046,224	Applicant(s)/Patent Under Reexamination NISHIOKA ET AL.	
	Examiner David G. Cervetti	Art Unit 2136	Page 2 of 3

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
	A	US-			
	B	US-			
	C	US-			
	D	US-			
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	Blum et al., Proving Security Against Chosen Ciphertext Attacks, 1990, Advances in Cryptology - CRYPTO '88, pp 256-268.
	V	Paillier et al., Efficient Public-Key Cryptosystems Provably Secure Against Active Adversaries, 1999, Springer-Verlag.
	W	David Pointcheval, Chosen-Ciphertext Security for Any One-Way Cryptosystem, 2000, Springer-Verlag, pp. 129-146.
	X	Victor Shoup, Using Hash Functions as a Hedge against Chosen Ciphertext Attack, May 9, 2000, IBM Zurich Research Lab.

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Notice of References Cited	Application/Control No. 10/046,224	Applicant(s)/Patent Under Reexamination NISHIOKA ET AL.	
	Examiner David G. Cervetti	Art Unit 2136	Page 3 of 3

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
	A	US-			
	B	US-			
	C	US-			
	D	US-			
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	Rivest et al., A method for obtaining digital signatures and public-key cryptosystems, Feb 1978, ACM, pp 120-126.
	V	Taher ElGamal, A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms, 1985, IEEE, vol 31, no. 4, pp. 469-472.
	W	Dan Boneh, The Decision Diffie-Hellman Problem, 1998, Springer-Verlag, pp. 48-63.
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.